# ABSTRACT

Cyber-Physical System Security (CPSs) enables Information Technology to be integrated with Operation Technology to efficiently monitor and manage the physical processes of various critical infrastructures. Recent incidents in cyber ecosystems have shown that CPSs are becoming increasingly vulnerable to complex attacks. These incidents often lead to sensing and actuation misbehaviour by illegal manipulations of data, which can severely impact the underlying physical processes of critical infrastructures. Current research acknowledges that IT-based security measures cannot entirely protect CPSs from such threats. Moreover, they are not designed to monitor the measurement level activities of physical processes, and they fail to mitigate blended cyber attacks, especially multi-stage and zero-day ones. This Project addresses these limitations by proposing a framework, named UnSupervised Misbehavior Detection (USMD), comprising a deep neural network that learns about a system's expected behavior from data-driven representations. USMD can identify in real-time the attacks on CPSs by using the long-short term memory and Attention method for multi-sensor data. The USMD's performance is evaluated on various known data sets (i.e., ToN_IoT, SWaT, WADI and Gas pipeline datasets). The experimental results indicate that the superior performance of USMD compared with six state-of-the-art methods, which we implemented and extensively tested. USMD achieves F-scores of 0.9699 and 0.9702 on SWaTand WADI datasets, respectively.